Alejandro Gomez

ITMS Security Audit

Incident Response

This was compared to NIST Generally Accepted Principles and Practices for Securing Information Technology Systems, Lesson 9 Documents (pg 31-36)

**IR0001 Security Incident Response Team Charter**

Recommendations/Concerns:

1. Version, Effective Date, Last Review, Next Review of policies are all old, it does not look like they have been looked at for some time.
2. **Priorities** were not mentioned in the business plan/write up.
3. Theft of data is not addressed in a **lengthy and extensive manner**, it is only discussed for validation purposes.
4. **Resources** that support critical functions are not clearly labeled or listed.

NIST policy 3.6.2 Identify Resources that following categories should be stated

* Time Frames needed
* Overlap of Areas
* Analyze Resources Needed
* Common Resources Used
* People
* Processing Capability (e.g., mainframes, personal computers)
* Computer-Based Services (e.g., telecommunications, world wide web)
* Data and Applications
* Physical Infrastructure Documents and Papers (e.g., documentation, blank forms, legal documents)

**IR0001.02 Information Security Incident Classification Matrix**

1. There is not a clear definition of “emergency” or “disaster” mentioned in the beginning policies. Would recommend that they are more clearly defined and create **contingency plans** of disasters to define actions during such events, as well as handling of critical resources during these.
2. Version, Effective Date, Last Review, Next Review of policies are all old, it does not look like they have been looked at for some time.
3. There should be a list of smaller and larger contingencies. Less obvious contingencies should be noted as well.
4. CP0002 \_Section 4: Has at least five different people maintaining the latest revision of the plans. This could be too many people and a conflict of roles and assigned jobs, would recommend reducing this number.

Policies IR0001.04 Security Incident Response Team Sequence of Actions, and IR0001.06 Information Security Incident Notification Schedule, are not available for review